有限体上の予想される第一原始多項式について

AUTHOR(S):

太刀川, 弘幸; 照井, 章

CITATION:

太刀川, 弘幸 ...[et al]. 有限体上の予想される第一原始多項式について. 数理解析研究所講究録 2009, 1652: 146-154

ISSUE DATE:

2009-06

URL:

http://hdl.handle.net/2433/140803

数理解析研究所講究録
第1652巻 2009年 146-154

The presupposed 1st primitive polynomials over a finite field
有限体上の予想される第一原始多項式について

太刀川 弘幸 *
HIROYUKI TACHIKAWA
照井 章 †
AKIRA TERUI
筑波大学大学院 数理物質科学研究科
GRADUATE SCHOOL OF PURE AND APPLIED SCIENCES, UNIVERSITY OF TSUKUBA

1 有限体上の第一原始多項式

$p \neq 0$ を素数、k, K を有限体 $GF(p), GF(p^m)$ とする。この場合、乗法群 $K \setminus \{0\}$ の生成元（複数）を K の原始元と呼び、原始元を根にもつ k 上の多項式を原始多項式 (primitive polynomial) という。ところで原始多項式は複数個存在する。そこでこれら複数の原始多項式にどのように番号を付けるかがこの発表の出発点である。

一つの原始多項式 (m 次の既約多項式でもある) を

$$f(x) = x^m - a_{m-1}x^{m-1} - a_{m-2}x^{m-2} - \cdots - a_0 \in k[x] \tag{1}$$

とする。$a_i \in k = GF(p) \simeq Z/(p)$ であるから、$0 \leq b_i \leq p-1$ で $a_i \equiv b_i \bmod p$ なる整数 b_i が一意的に存在する。そこで、$n_f := b_{m-1}p^{m-1} + \cdots + b_0 \in Z$ を $f(x)$ の番号としようというのが我々の提案である。更にこの番号付けは m 次の全ての（既約とは限らない）k 上多項式（$p^m - 1$ 個）に対しても適用する。

集合 $\{0, 1, \cdots, p^m - 1\}$ の部分集合 $\{n_f | f(x)$ は原始 t 多項式 $\}$ を Σ と置く。そして、Σ の中で最小の n_f を番号にもつ原始多項式を K の第一原始多項式（1st primitive polynomial, 略して 1st pp）と呼ぶことにするのである。

予想 1
充分大なる m に対し 集合 Σ は 集合 $\{1, \cdots, p^m - 1\}$ の中で *at random* に分布している。

注意 1
原始多項式は擬似乱数 *(pseudo random numbers)* の作成に利用されているが、その集合は Σ とは異なる。

*pytha345@mail2.accsnet.ne.jp
†terui@math.tsukuba.ac.jp

この予想 1 が成立すると仮定すると次の結果を導くことができる。

α を一つの原始元とすれば、Galois 理論から $K=\{\alpha,\alpha^2.\cdots,1(=\alpha^{p^m-1}),0\}$ としてよい。更に α^r を abel 乗法群 $K\setminus\{0\}$ の生成元とすれば、$\gcd(k,p^m-1)=1$. 従って K の原始元の個数は $\varphi(p^m-1)$, 但し φ は Euler 関数である。そのうち m 個の共役元が一つの原始多項式を形成するから、異なる原始多項式の個数は $\dfrac{\varphi(p^m-1)}{m}$ となる。

従って予想 1 が正しいと仮定すれば、第一原始多項式 $f(x)$ に対して $n_f\approx\dfrac{\frac{p^m-1}{\varphi(p^m-1)}}{m}=\dfrac{m(p^m-1)}{\varphi(p^m-1)}$ と予想される。実は表題の the 1st presupposed primitive polynomial (略して 1st ppp) はこのような多項式を指す。

ここで 1st pp と 1st ppp を比較する為に $p=2$ の場合ではあるが、34 次までの殆ど全ての既約多項式が載っている Peterson,W.W. and Weldon, E.J.: Error-Correcting Codes, 2nd ed. MIT Press (1972) [9] を選ぶことにしよう (次頁表 1)。

ところで、表 1 の中で $m=14$, 1st pp = 63(43) と記しているところは、数式処理システム GAL (General Algebraic Language/Laboratory) で記述した自作の procedure を使って計算した結果、63 は真の 1st pp でないことが判明し、43 に修正したものである。このような修正が 8 例もあったことは大変意外であった。

この表で、不等式 1st pp < 1st ppp の成立している場合は 16、等式 1st pp = 1st ppp の成立している場合は 2、不等式 1st pp > 1st ppp の成立している場合は 15 である。我々の予想 1 がほぼ成立していると判断できそうな結果である。

2 第一原始多項式を求めるアルゴリズム

ここで簡単な procedure を作るための algorithm の説明に入ろう。所謂 Shift Register Algorithm ([5], [7]) と呼ばれているものの典型的な一つで、番号付 n_f を採用する根拠の一つを与えるものである。

式 (1) に戻ろう。このとき同形

$$\epsilon:K=k\alpha^{m-1}\oplus k\alpha^{m-2}\oplus\cdots\oplus k\simeq k[x]/(f(x))=k^m$$

が存在している。ここでは、$k[x]/(f(x))$ を k 上 m 次元空間と見做している。又、1 対 1 写像

$$\text{adic}:Z\ni n=a_{m-1}p^{m-1}+a_{m-2}p^{m-2}+\cdots+a_0\longmapsto(a_{m-1},a_{m-2},\cdots,a_0)\in k^m,$$
$$0\le a_i\le p-1,i=1,2,\cdots,m-1$$

も定義しておく。

そして、対応 $K\xrightarrow{\epsilon}k^m$ (k 上の m 次元ベクトル空間) $\xleftarrow{\text{adic}}$ m 桁の p-進数の集合:

$$u_{m-1}\alpha^{m-1}+u_{m-2}\alpha^{m-2}+\cdots+u_0\xmapsto{\epsilon}(u_{m-1},u_{m-2},\cdots,u_0)\xmapsto{\text{adic}}u_{m-1}p^{m-1}+u_{m-2}p^{m-2}+\cdots+u_0,u_i\in k$$

を考えることができる。

m	1st pp	2^m-1	$\frac{2^m-1}{\varphi(2^m-1)}$	1st ppp
2	3	3	1.50	3
3	3	7	1.17	4
4	3	$3\cdot 5$	1.88	8
5	5	31	1.03	5
6	3	$3^2\cdot 7$	1.75	11
7	3	127	1.01	7
8	29	$3\cdot 5\cdot 17$	1.99	16
9	17	$7\cdot 7$	1.18	11
10	9	$3\cdot 11\cdot 31=1023$	1.71	17
11	5	$23\cdot 89=2047$	1.06	12
12	83	$3^2\cdot 5\cdot 7\cdot 13=4095$	2.37	28
13	27	8191	1.00	13
14	63(43)	$3\cdot 43\cdot 127=16383$	1.54	22
15	3	$7\cdot 31\cdot 151=32767$	1.21	18
16	57(45)	$3\cdot 5\cdot 17\cdot 257=65535$	2.00	32
17	9	131071	1.00	17
18	129(39)	$3^3\cdot 7\cdot 19\cdot 73$	1.87	34
19	39	524287	1.00	19
20	9	$3\cdot 5^2\cdot 11\cdot 31\cdot 41$	2.18	44
21	5	$7^2\cdot 127\cdot 337$	1.18	25
22	3	$3\cdot 23\cdot 89\cdot 683$	1.59	35
23	33	$47\cdot 178481$	1.02	23
24	135(27)	$3^2\cdot 5\cdot 7\cdot 13\cdot 17\cdot 241$	2.53	61
25	9	$31\cdot 601\cdot 1801$	1.04	26
26	71	$3\cdot 2731\cdot 8191$	1.50	39
27	39	$7\cdot 73\cdot 262657$	1.18	32
28	9	$3\cdot 5\cdot 29\cdot 43\cdot 113\cdot 127$	2.02	57
29	5	$233\cdot 1103\cdot 2089$	1.01	29
30	8388615(83)	$3^2\cdot 7\cdot 11\cdot 31\cdot 151\cdot 331$	2.01	60
31	9	2147483647	1.00	31
32	300811(175)	$3\cdot 5\cdot 17\cdot 257\cdot 65537$	2.00	64
33	8193(83)	$7\cdot 23\cdot 89\cdot 599479$	1.23	41
34	134217735(231)	$3\cdot 43691\cdot 131071$	1.50	51

表 1: 1st pp と 1st ppp の表 (Peterson, W.W. and Weldon, E.J. [9]).

特に上の対応で

$$1 \overset{\epsilon}{\longmapsto} (0,0,\cdots,0,0,1) \overset{\text{adic}}{\longmapsto} 1;$$
$$\alpha \overset{\epsilon}{\longmapsto} (0,0,\cdots,0,1,0) \overset{\text{adic}}{\longmapsto} p;$$
$$\alpha^2 \overset{\epsilon}{\longmapsto} (0,0,\cdots,1,0,0) \overset{\text{adic}}{\longmapsto} p^2;$$
$$\vdots$$
$$\alpha^{m-1} \overset{\epsilon}{\longmapsto} (1,0,\cdots,0,0,0) \overset{\text{adic}}{\longmapsto} p^{m-1};$$
$$\alpha^m \overset{\epsilon}{\longmapsto} (a_{m-1},a_{m-2},\cdots,a_0) \overset{\text{adic}}{\longmapsto} a_{m-1}p^{m-1}+a_{m-2}p^{m-2}+\cdots+a_0;$$
$$\alpha^{m+1} \overset{\epsilon}{\longmapsto} (a_{m-1}^2+a_{m-2}, a_{m-1}a_{m-2}+a_{m-3},\cdots,a_{m-1}a_1+a_0, a_{m-1}a_0)$$
$$\overset{\text{adic}}{\longmapsto} (a_{m-1}^2+a_{m-2})p^{m-1}+(a_{m-1}a_{m-2}+a_{m-3})p^{m-2}+\cdots+(a_{m-1}a_1-a_0)p+a_{m-1}a_0;$$
$$\vdots$$

である。 一般に $\alpha^i = k_{m-1}\alpha^{m-1}+k_{m-2}\alpha^{m-2}+\cdots+k_1\alpha+k_0$, $1 \le i \le p^m-1$ に対して

$$\begin{aligned}\alpha^{i+1} &= \alpha(k_{m-1}\alpha^{m-1}+k_{m-2}\alpha^{m-2}+\cdots+k_1\alpha+k_0)\\ &= k_{m-1}\alpha^m+k_{m-2}\alpha^{m-1}+\cdots+k_1\alpha^2+k_0\alpha\\ &= k_{m-1}(a_{m-1}\alpha^{m-1}+a_{m-2}\alpha^{m-2}+\cdots+a_1\alpha+a_0)+k_{m-2}\alpha^{m-1}+\cdots+k_1\alpha^2+k_0\alpha\\ &= (k_{m-1}a_{m-1}+k_{m-2})\alpha^{m-1}+(k_{m-1}a_{m-2}+k_{m-3})\alpha^{m-2}+\cdots+(k_{m-1}a_1+k_0)\alpha+(k_{m-1}a_0)\end{aligned}$$

であるから、 α^{i+1} の p-進数表示は

$$(k_{m-1}a_{m-1}+k_{m-2}, k_{m-1}a_{m-2}+k_{m-3},\cdots,k_{m-1}a_1+k_0, k_{m-1}a_0)$$

である。

そこで、ベクトル空間の間の関数 τ_f を

$$\tau_f((k_{m-1},k_{m-2},\cdots,k_0)) = (k_{m-1}a_{m-1}+k_{m-2}, k_{m-1}a_{m-2}+k_{m-3},\cdots,k_{m-1}a_1+k_0, k_{m-1}a_0)$$

で定義する。τ_f は τ_A と記すこともある、但し A は $(a_m,a_{m-1},\cdots,a_0) = \text{adic}(n_f)$ のことである。

この関数 τ_f は procedure の中に implement することは容易である。また、上の解説の第 m 行 は $\alpha^m \overset{\epsilon}{\longmapsto} (a_{m-1},a_{m-2},\cdots,a_0) = \tau_f^m(\text{adic}(1))$ であることを注意しておく。

ところで、α が原始根であるための必要十分条件は、等式 $K-\{0\} = \{\alpha,\alpha^2,\cdots,\alpha^{p^m-1}(=1)\}$ の成立することである。従って上の α^i に対応する $\tau_f^i(\text{adic}(1))$ が重複無く現れてくる必要がある。その個数は p^m-1 で、又その時に限り $f(x)$ は原始多項式になるといえる。

さて、ここで一般の m 次多項式 $g(x) \in k[x]$ を考えてみる。

$$g(x) = x^m+c_{m-1}x^{m-1}+c_{m-2}x^{m-2}+\cdots+c_0 \tag{2}$$

とおく。前述の記号を拡張して踏襲すれば $\tau_g = \tau_{\text{adic}(n_g)}$ であり、$\text{adic}(n_g) = (c_{m-1},c_{m-2},\cdots,c_0)$ である。又 前述の adic の定義から明らかに $\text{adic}(1) = (0,0,\cdots,1)$ である。

$g(x)=0$ の根を β とすれば、$f(x)$ の場合と全く同様に $\{\beta,\beta^2,\cdots,\beta^{p^m-1}\}$ に対応する m 次のベクトルの列 $\tau_g(\text{adic}(1)), \tau_g^2(\text{adic}(1)),\cdots,\tau_g^{p^m-1}(\text{adic}(1))$ が現れてくるが、$g(x)$ が原始で無いとすれば、適当な $1 \le i < j \le p^m-1$ で $\tau_g^i(\text{adic}(1)) = \tau_g^j(\text{adic}(1))$ となる。このとき $s = \min\{j-i\}$ を g (或いは $\text{adic}(n_g)$) の 周期 (period) と呼ぶ。再び 原始多項式 $f(x)$ にもどれば τ_f の周期は p^m-1 であると言える。 Cf. [2].

周期に関して計算の時間を短縮する都合の良い次の補題がある。

補題 1
g の周期を $s=k-j$ とするとき、$1 \leq l \leq m$ なる整数 l が一意的に存在して $\tau_g^i(\mathrm{adic}(1)) = \tau_g^j(\mathrm{adic}(1)) = \tau_g^l(\mathrm{adic}(1))$ が成立する。

そこで、我々の 1st pp を求めるアルゴリズムは "$\tau_{\mathrm{adic}(1)}$ の周期, $\tau_{\mathrm{adic}(2)}$ の周期, ... と進んで行き, 初めに $\tau_{\mathrm{adic}(n)}$ の周期が p^m-1 となったとき、ベクトル $\mathrm{adic}(n)$ の座標を $m-1$ 次以下の項としてもつ m 次 monomial な 多項式が 1st pp" と言える。 従って n を求める procedure はアルゴリズム 1 のようになる。({} の中の文はコメントを表す。)

アルゴリズム 1 (1st pp の計算)
Input: p, m
Output: n {1st pp f の番号 n_f}
1: **for all** $i=1,\ldots,p^m-1$ **do** {$i=n_f$, f: $\alpha \in K$ の定義多項式 }
2: **for all** $j=m+1,\ldots,p^m-1$ **do** {α^j を計算 }
3: **if** $\tau_{\mathrm{adic}(i)}(\mathrm{adic}(j)) \in \{\mathrm{adic}(1), \mathrm{adic}(2), \ldots, \mathrm{adic}(m)\}$ **then**
4: $n \longleftarrow j$; { 補題 1 がみたされるならば, α の周期は j}
5: for ループから出る;
6: **end if**
7: **end for**
8: **if** $n=p^m-1$ **then** {α の周期が $p^m-1 \Longleftrightarrow \alpha$ は原始元のとき }
9: $n \longleftarrow i$; {$n_f=i$ なる f が k 上の 1st pp}
10: for ループから出る;
11: **end if**
12: **end for**
13: **return** n;

3 第一原始多項式の時間計算量に関する予想

ところで、n は上に紹介した procedure で原始多項式に到達する最小の時間を与えることになる。従って、この時間が m の多項式で近似できるかどうかが、第一原始多項式の Complexity 問題と言うことができる。つまり、若し我々の予想 1 が正しいとして

問題 1
$C = \lim_{m\to\infty} m\dfrac{p^m-1}{\varphi(p^m-1)}$ は m の 多項式で近似できるか?

$p=2$ の場合であるが、表 1 の $\dfrac{2^m-1}{\varphi(2^m-1)}$ はかなり小であるので、$\lim_{m\to\infty} \dfrac{2^m-1}{\varphi(2^m-1)} < \infty$ ではないだろうか?という疑問が湧く。若し正しいとすれば、第一原始多項式 1st pp の Complexity が m に関して linear, 即ち, $C \sim O(m)$, であると言うことになる。然しそれは次の定理 1 によって否定される。

定理 1
$L = \lim_{m\to\infty} \dfrac{2^m-1}{\varphi(2^m-1)}$ は有界とは限らない。

証明 整数 3 からはじまり次々に素数をならべて r 番目が q_r であるとする。即ち $3=q_1<q_2<\cdots<q_r$ は素数の列とする。

更に m は等式 $m=(q_1-1)(q_2-1)\cdots(q_r-1)$ を満たす整数とする。$r\to\infty$ のとき、勿論 $m\to\infty$ である。このような $m\to\infty$ に対し、極限 $\lim_{m\to\infty}\frac{2^m-1}{\varphi(2^m-1)}$ を計算してみよう。

$q_j\neq 2$ であるから Fermat の小定理により $q_j|2^{q_j-1}-1$ for $j=1,2,\cdots,r$ 更に $2^{q_j-1}-1|2^m-1$ for $j=1,2,\cdots,r$ であるから $q_j-1|m$ ならば $q_j|2^m-1$ 従って $2^m-1=q_1^{c_1}q_2^{c_2}\cdots q_r^{c_r}q_{r+1}^{c_{r+1}}\cdots q_s^{c_s}$ for $r\leq s$, しかも $1\leq c_i$ for $1\leq i\leq r$ が成立する。故に

$$\begin{aligned}\frac{2^m-1}{\varphi(2^m-1)}&=\left\{\frac{1}{(1-\frac{1}{q_1})}\frac{1}{(1-\frac{1}{q_2})}\cdots\frac{1}{(1-\frac{1}{q_r})}\right\}\left\{\frac{1}{(1-\frac{1}{q_{r+1}})}\cdots\frac{1}{(1-\frac{1}{q_s})}\right\}\\&\geq\frac{1}{(1-\frac{1}{q_1})}\frac{1}{(1-\frac{1}{q_2})}\cdots\frac{1}{(1-\frac{1}{q_r})}\\&=\left(1+\frac{1}{q_1}+\frac{1}{q_1^2}+\cdots\right)\left(1+\frac{1}{q_2}+\frac{1}{q_2^2}+\cdots\right)\cdots\left(1+\frac{1}{q_r}+\frac{1}{q_r^2}+\cdots\right)\\&=\sum_{(a_1,a_2,\cdots,a_r)}\frac{1}{q_1^{a_1}q_2^{a_2}\cdots q_r^{a_r}}\end{aligned}$$

そこで

$$\lim_{m\to\infty}\frac{2^m-1}{\varphi(2^m-1)}=\lim_{r\to\infty}\sum_{(a_1=0,a_2=0,\cdots,a_r=0)}^{(\infty,\infty,\cdots,\infty)}\frac{1}{q_1^{a_1}}\frac{1}{q_2^{a_2}}\cdots\frac{1}{q_r^{a_r}}$$

を一時的に L と置いてみよう。任意の正の整数 n は適当な s,r に対して一意的に $n=2^s q_1^{a_1}q_2^{a_2}\cdots q_r^{a_r}$ と表されるから $1+\frac{1}{2}+\cdots+\frac{1}{n}+\cdots=L+\frac{1}{2}L+\cdots+\frac{1}{2^s}L+\cdots=\frac{1}{1-\frac{1}{2}}L=2L.$ $1+\frac{1}{2}+\cdots+\frac{1}{n}+\cdots$ が有界で無いから、$L=\lim_{m\to\infty}\frac{2^m-1}{\varphi(2^m-1)}$ も有界ではない。 ∎

さて $L=\lim_{m\to\infty}\frac{2^m-1}{\varphi(2^m-1)}$ が有界である場合として 2^m-1 が素数である場合が考えられる。有名な Mersenne 素数の場合である。Mersenne 素数が無限個存在することは未だ証明されていない。従って L の素数 $(2^m-1)\to\infty$ に対する極限を考えることは無意味である。然し Mersenne 数なら、即ち L の素数 $m\to\infty$ に対する極限を考えることは意味がある。そして次の定理を得る。

定理 2

$L=\lim_{\text{素数}\ m\to\infty}\frac{2^m-1}{\varphi(2^m-1)}=1$, 即ち、素数 $m\to\infty$ に対し $C\sim O(m)$.

証明 p を 2 と異なる素数とする。更に Mersenne 数 $M_p=2^p-1$ の任意の素数因子を q とする。$q|2^p-1$, 即ち $2^p\equiv 1 \bmod q$. そこで、乗法群 $Z/(q)\setminus\{0+(q)\}$ の元 $2 \bmod q$ の位数を h とすれば $h|p$, 然し p は素数であるから $h=p$. さて、フェルマーの小定理から $2^{q-1}\equiv 1 \bmod q$, 従って $p|q-1$, 故に $k'=\frac{q-1}{p}$ とおけば $q-1=k'p$. 一方、$q-1$ は偶数であり、$p\neq 2$ であるから整数 k が存在して $q=2kp+1$ となる。

次に $2^p-1=\prod_{i=1}^{t}q_i^{r_i}$, 但し q_i は素数とする。勿論 $q_i\neq 2$. このとき $\varphi(2^p-1)=\prod_{i=1}^{t}\varphi(q_i^{r_i})=\prod_{i=1}^{t}q_i^{r_i}\left(1-\frac{1}{q_i}\right)$. $q_1<q_2<\ldots<q_t$ と仮定すれば、前述の説明から $q_i=2k_ip+1$ と置ける。従って

$$(2p+1)^t\leq(2k_1p+1)^t\leq\prod_{i+1}^{t}(2k_ip+1)^{r_i}=2^p-1.$$

これから、更に $(2p)^t<2^p$ として良い。従って $t<\frac{p}{1+\log_2 p}$.

そこで $\lim_{\text{素数}\ p\to\infty}\frac{2^p-1}{\varphi(2^p-1)}=\prod_{i=1}^{t}\left(1-\frac{1}{q_i}\right)^{-1}<\left(1-\frac{1}{q_1}\right)^{-t}=\left(1+\frac{1}{2k_1p}\right)^t<\left(1+\frac{1}{2p}\right)^{\frac{p}{1+\log_2 p}}$.

計算のため $s := \log_2 p$ とおけば $\left(1+\frac{1}{2p}\right)^{\frac{p}{1+\log_2 p}} = \left(1+\frac{1}{2^{s+1}}\right)^{\frac{2^s}{1+s}}$ であり、$p \to \infty$ ならば $s \to \infty$ である。 従って $\lim_{\text{素数 } p\to\infty} \frac{2^p-1}{\varphi(2^p-1)} = \lim_{s\to\infty}\left(1+\frac{1}{2^{s+1}}\right)^{\frac{2^{s+1}}{2(1+s)}} = \lim_{s\to\infty} e^{\frac{1}{2(1+s)}} = 1.$ ∎

次に、Conway [4] の代数閉体 On_2 の部分体 $GF(2^{2^t})$ に対し $\lim_{t\to\infty}\frac{1}{2^{2^t}}\frac{2^{2^t}-1}{\varphi(2^{2^t}-1)}$ を計算してみよう。

定理 3
$\lim_{t\to\infty}\frac{1}{2^{2^t}}\frac{2^{2^t}-1}{\varphi(2^{2^t}-1)} = 0$, 即ち、体 On_2 の部分体達に対し $C \sim o(m^2)$ である。

証明 先ず因数分解 $2^{2^t}-1 = (2^{2^{(t-1)}}-1)(2^{2^{(t-1)}}+1)$ が成立する。次に $2^{2^{(t-1)}}-1$ と $2^{2^{(t-1)}}+1$ との共通素因子は存在しない。何故なら, c を一つの共通素因子とすれば $2^{2^{(t-1)}} \equiv 1 \bmod c$, 且つ $2^{2^{(t-1)}} \equiv -1 \bmod c$. 従って $1-(-1) = 2 \equiv 0 \bmod c$. 故に $c = 2$ より矛盾。

さて $2^{2^{(t-1)}}+1$ の因子となる一つの素数 q をとると、初の因数分解から q は $2^{2^t}-1$ の因子であり、$2^{2^t} \equiv 1 \bmod q$ が成立。一方、乗法群 $Z/(q)\setminus\{0+(q)\}$ の元 $2+(q)$ の位数を g とすれば $g|2^t$ であるから、或る $1 \le i \le t$ に対して $g = 2^i$ が成立。 同様に、若し q が $2^{2^{(t-1)}}-1$ の素因子であれば、或る $1 \le j \le t-1$ が存在して、$g = 2^j$ が成立する。従って、$2^{2^t}-1$ の素因子で $2^{2^{(t-1)}}-1$ の素因子でない、即ち $2^{2^{(t-1)}}+1$ の素因子である為には $g = 2^t$ となる。 他方 Fermat の小定理から $g|(q-1)$, 従って整数 k が存在して $q = kg+1 = k2^t+1$.

初めの因数分解より、このような q は $2^{2^{(t-1)}}+1$ の素因子でなければならないし、逆に $2^{2^{(t-1)}}+1$ の素因子はこのような表現 $k2^t+1$ を持つ。

ここで $2^{2^{(t-1)}}+1$ の素因子を次のように取る。$2 \neq q_1 < q_2 < \cdots < q_s$. このとき、$s \ge i \ge 1$ に対し、$2^{2^{(t-1)}}+1 = q_1^{r_1}q_2^{r_2}\cdots q_s^{r_s}$, $r_i \ge 1$, とおける。

前述の結果より、任意の i に対し $2^t+1 \le q_i$, 故に $(2^t+1)^{r_1+r_2+\cdots+r_s} \le 2^{2^{(t-1)}}+1$ が成立。

$r = r_1+r_2+\cdots+r_s$ とおけば $(2^t)^r \le 2^{2^{(t-1)}}$. 故に $tr\log_2 2 \le 2^{(t-1)}\log_2 2 \Longrightarrow r \le \frac{2^{(t-1)}}{t} \Longrightarrow s \le \frac{2^{(t-1)}}{t}$.

さて

$$\frac{2^{2^{(t-1)}}+1}{\varphi(2^{2^{(t-1)}}+1)} = \prod_{i=1}^{s}\frac{q_i}{q_i-1} \le \left\{\frac{1}{1-\frac{1}{q_1}}\right\}^s \le \left\{\frac{1}{1-\frac{1}{2^t}}\right\}^s \le \left\{\frac{1}{1-\frac{1}{2^t}}\right\}^{\frac{2^{(t-1)}}{t}} \le e^{\frac{1}{2^t}\frac{2^{(t-1)}}{t}} = e^{\frac{1}{2t}}.$$

従って $\frac{2^{2^t}-1}{\varphi(2^{2^t}-1)} = \prod_{u=0}^{t-1}\frac{2^{2^u}+1}{\varphi(2^{2^u}+1)} \le e^{\frac{1}{2}(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{u})}$, 故に

$$\lim_{t\to\infty}\frac{1}{2^t}\frac{2^{2^t}-1}{\varphi(2^{2^t}-1)} \le \lim_{t\to\infty} e^{-t\log 2}e^{\frac{1}{2}(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{t})}$$
$$= \lim_{t\to\infty} e^{\frac{1}{2}(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{t}-\log t)}e^{\frac{1}{2}(\log t-2t\log 2)} = \lim_{t\to\infty} e^{\frac{1}{2}(\gamma+(\log t-2t\log 2))}.$$

ここで γ は Euler の定数である。ところで $\lim_{t\to\infty}(\log t - 2t\log 2) = -\infty$, (何故なら $f(t) = \log t - 2t\log 2$ に対し, $f(1) = -2\log 2 < 0, f'(t) = \frac{1}{t} - 2\log 2 < 0$ for $1 < t$ であるから), 結局 $\lim_{t\to\infty}\frac{1}{2^t}\frac{2^{2^t}-1}{\varphi(2^{2^t}-1)} = 0$. ∎

上の証明で Euler の定数 $\gamma = \lim_{t\to\infty} 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{t}-\log t$ が登場してくるところは興味深い。Cf. 高木貞治著: 解析概論 (岩波書店) [15, p. 150].

又、定理 3 は、任意の素数 q に対して $\lim_{t\to\infty}\frac{1}{q^t}\frac{2^{q^t}-1}{\varphi(2^{q^t}-1)}=0$ の成立という形で拡張される。

追記 本稿 表 1 は Peterson-Weldon [9] から引用したものであるが、多項式の表記は各項の位置を three binary digits で記述してあるので、我々の記述に直すにはとても時間を要した。調べて行くうちに、文献 ([1], [3], [6], [8], [10], [11], [13], [14]) のように非常に次数の高い原始多項式の載っているデータが多数存在することが分ったが、その中に今回発表している数字 n_f で多項式を表記する試みは一つもなかった。多分 N. Zierler and J. Brillhart ([13], [14]) の影響か、3 項 (trinomial) の原始多項式、あるいは、符号理論 ([2], [9]) の影響か、項の少ない (weight の低い) 原始多項式が調べられていた。勿論、殆どが 1st pp でない、これが今回の発表を促すことに繋がった。

既に注意したように、原始多項式が擬似乱数の作成に利用されている。$\alpha\in GF(2^m)$ を一つの原始多項式 $x^m-c_{m-1}x^{m-2}-\cdots-c_0\in GF(2)$ の根とするとき、列 $\epsilon(\alpha),\epsilon(\alpha^2),\cdots,\epsilon(\alpha^{2^m-1})$ を random bit と呼んでいる。Σ は 原始多項式達の分布であるから random bit とは異なる。

4 今後の研究課題

1. 予想 1 の成立を検討するために Σ の分布を研究する。一つの試みとして、より高次な第一原始多項式を求めてゆく必要がある。従って、より計算時間の少ない procedure の開発、研究を行うつもりである ([2], [7])。
2. 定理 2 は、$p\neq 2$ の場合、$\lim_{\text{素数 } m\to\infty}\frac{p^m-1}{\varphi(p^m-1)}=1$ と拡張される。この発表で述べた予想, 問題, 定理を標数 $p\neq 2$ の場合に拡張したい [12]。

参 考 文 献

[1] P. H. Bardell. Primitive polynomials of degree 301 through 500. *Journal of Electronic Testing: Theory and Applications*, Vol. 3, pp. 175–176, 1992.

[2] E. R. Berlekamp. *Algebraic Coding Theory.* McGraw-Hill Book Co., New York, 1968.

[3] R. P. Brent, S. Larvala, and P. Zimmermann. A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377. *Math. Comp.*, Vol. 72, No. 243, pp. 1443–1452 (electronic), 2003.

[4] J. H. Conway. *On Numbers and Games.* Academic Press, 1976. London Mathematical Society Monographs, No. 6.

[5] S. W. Golomb. *Shift Register Sequences.* Aegean Park Press, Laguna Hills, CA, USA, 1981.

[6] T. Hansen and G. L. Mullen. Primitive polynomials over finite fields. *Math. Comp.*, Vol. 59, No. 200, pp. 639–643, S47–S50, 1992.

[7] D. E. Knuth. *The Art of Computer Programming.* Addison-Wesley, 3rd edition, 1997. Volume 1: Fundamental algorithms.

[8] R. Lidl and H. Niederreiter. *Finite Fields*, Vol. 20 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, 2nd edition, 1997.

[9] W. W. Peterson and E. J. Weldon, Jr. *Error-correcting codes.* The M.I.T. Press, Cambridge, Mass.-London, 2nd edition, 1972.

[10] J. Rajski and J. Tyszer. Primitive polynomials over $GF(2)$ of degree up to 660 with uniformly distributed coefficients. *J. Electronic Testing*, Vol. 19, No. 6, pp. 645–657, December 2003.

[11] W. Stahnke. Primitive binary polynomials. *Math. Comp.*, Vol. 27, pp. 977–980, 1973.

[12] E. Sugimoto. A short note on new indexing polynomials of finite fields. *Inform. and Control*, Vol. 41, No. 2, pp. 243–246, 1979.

[13] N. Zierler and J. Brillhart. On primitive trinomials (mod 2). *Information and Control*, Vol. 13, pp. 541–554, 1968.

[14] N. Zierler and J. Brillhart. On primitive trinomials (mod 2). II. *Information and Control*, Vol. 14, pp. 566–569, 1969.

[15] 高木貞治. 解析概論（改訂第 3 版）. 岩波書店, 1983.